Model-Based Integration Of Embedded Software

PI Meeting

July 24 – 26, 2002
New York, NY

Smart Vehicles: Expanded Challenge Problem Definition

Anouck Girard, anouck@eecs.berkeley.edu

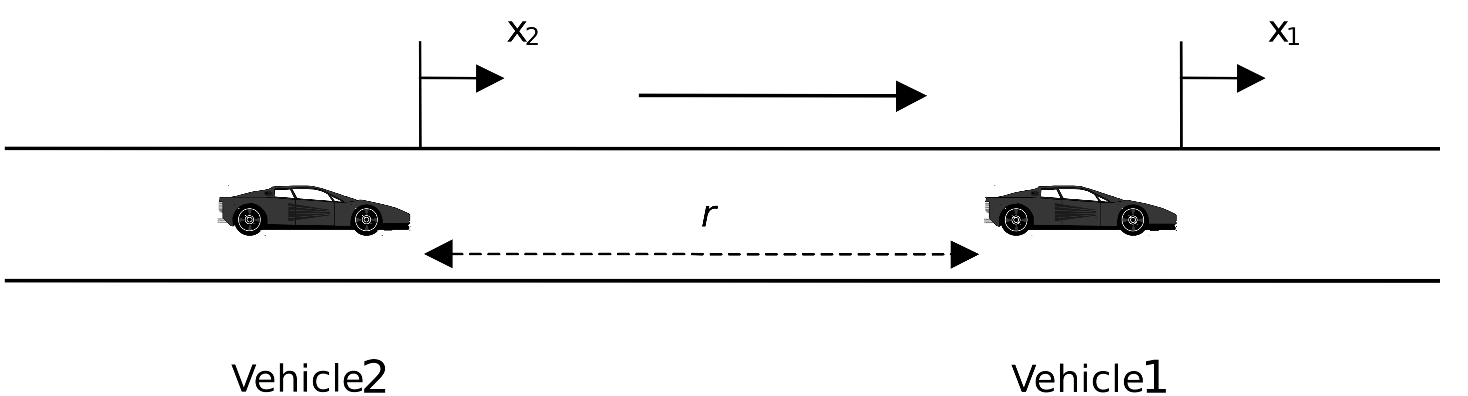
The University of California, Berkeley

Contract Number: F33615-00-C-1698
Award End Date: 31 Dec 03

Baseline Demo

Cooperative Adaptive Cruise Control with Collision Warning (CACC + CW)

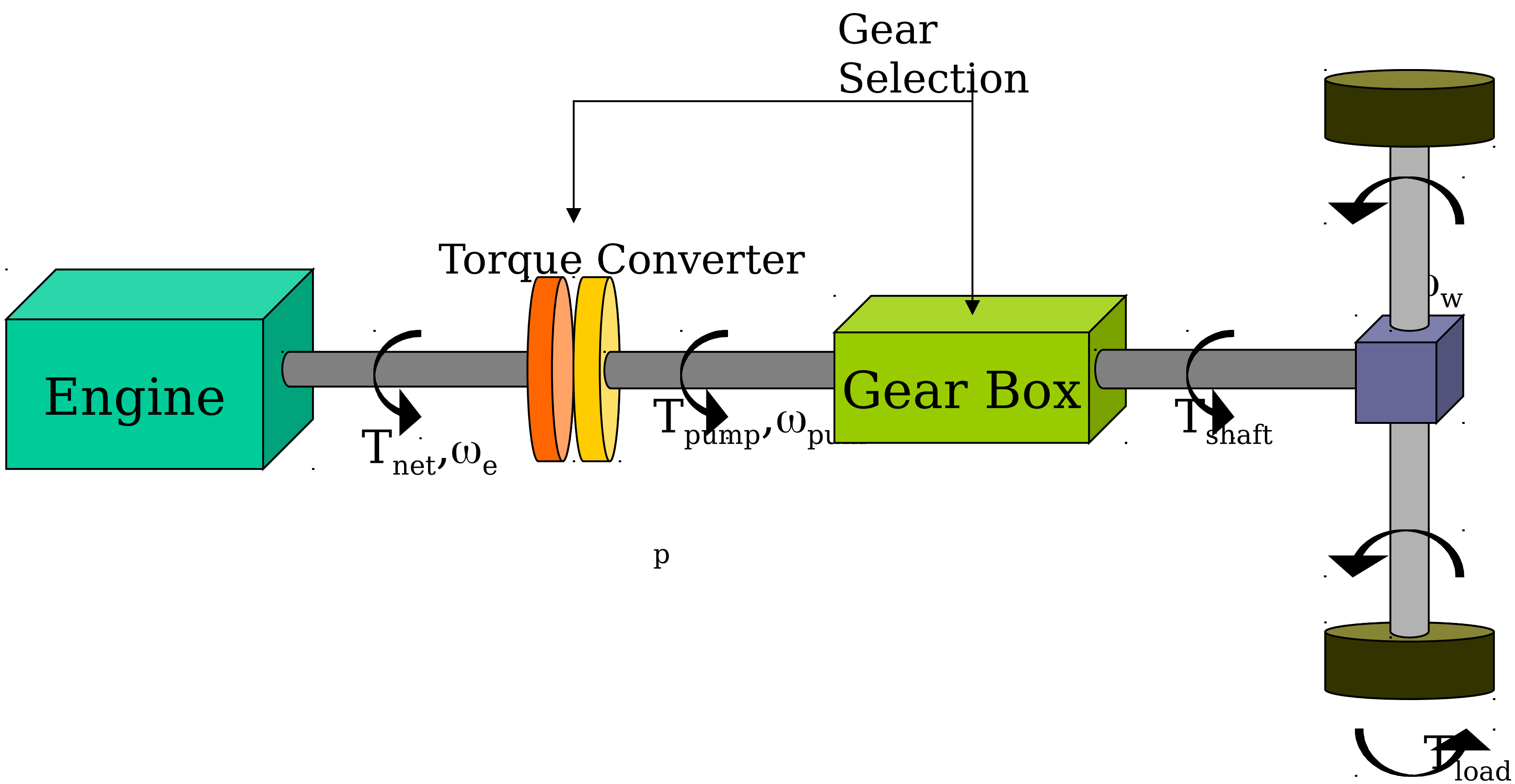
- **CACC:** Cruise at given speed when the road is clear (cruise control) , otherwise follow the car in front, using radar (adaptive) and/or communications (cooperative).
- **CW:** Warn the driver when an object is being approached too fast, or is too close.



Available Hardware

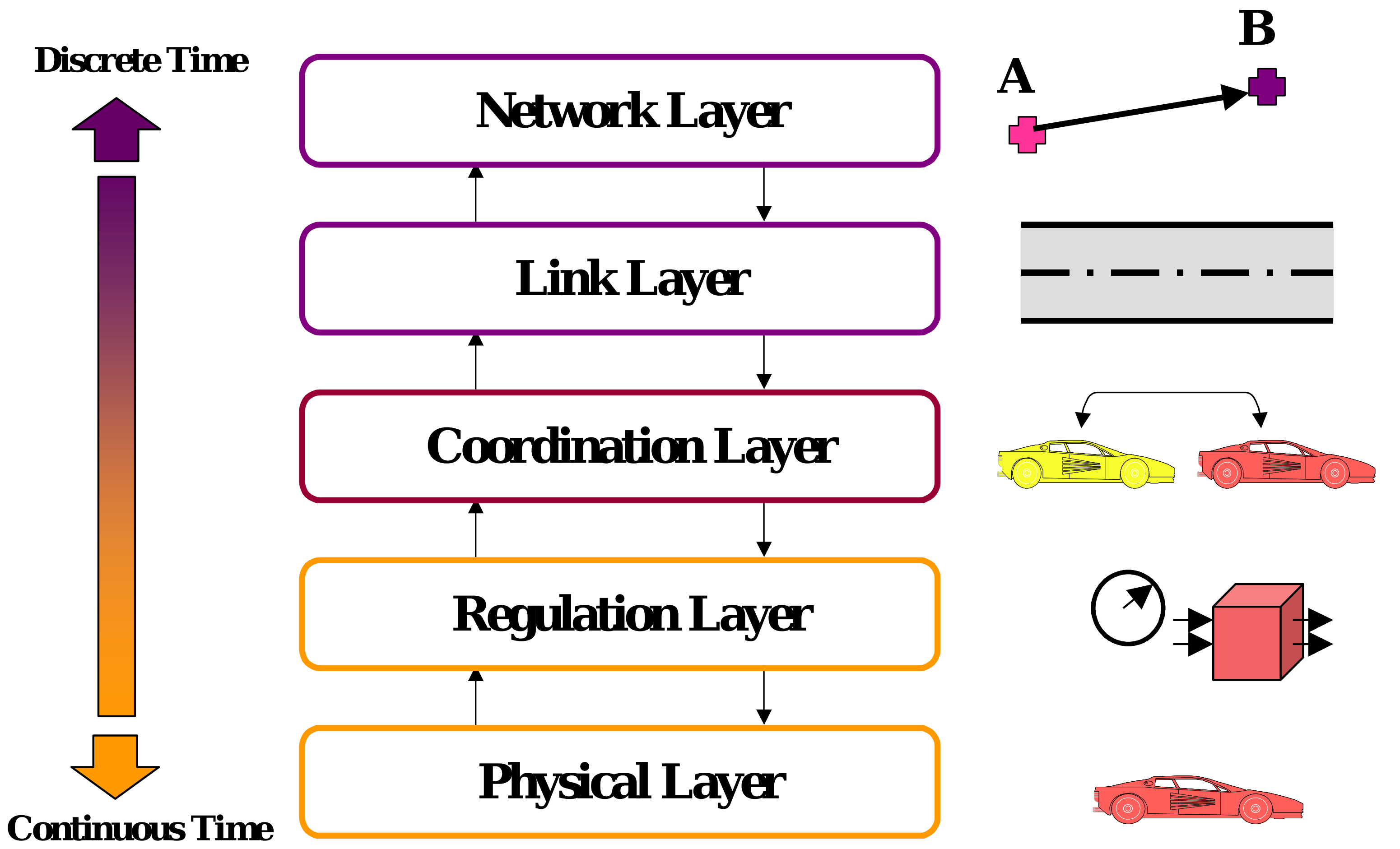
- Radar tracking up to 7 targets in FCM, giving distance, relative speed, and azimuth for each.
- Vision or radar for detection of stationary objects.
- Wireless communication (based on 802.11 or Token Bus).

Vehicle Model

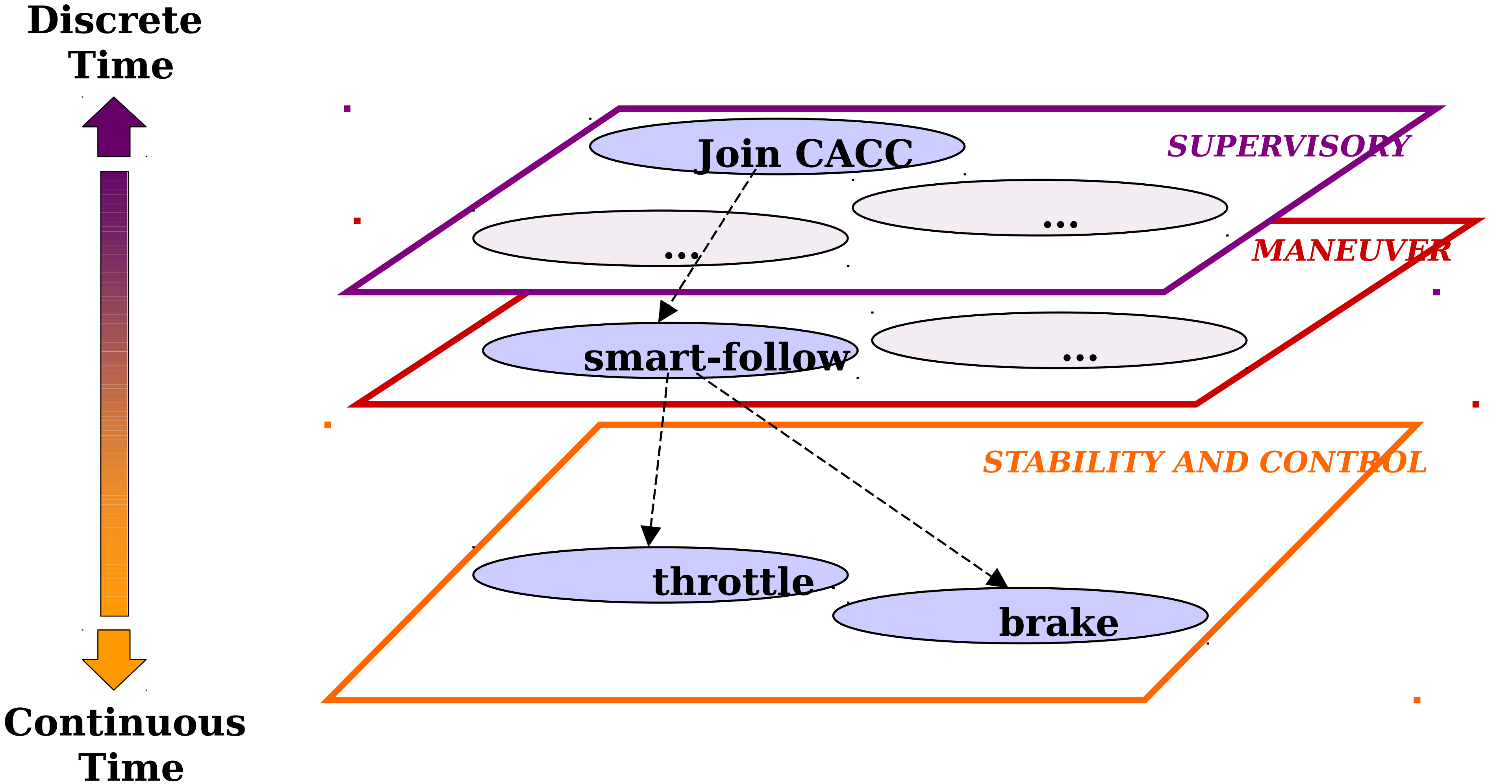


Reference is paper by Cho and Hedrick:
http://vehicle.me.berkeley.edu/mobies/powertrain/models/autotool/asme-mo

The PATH Architecture



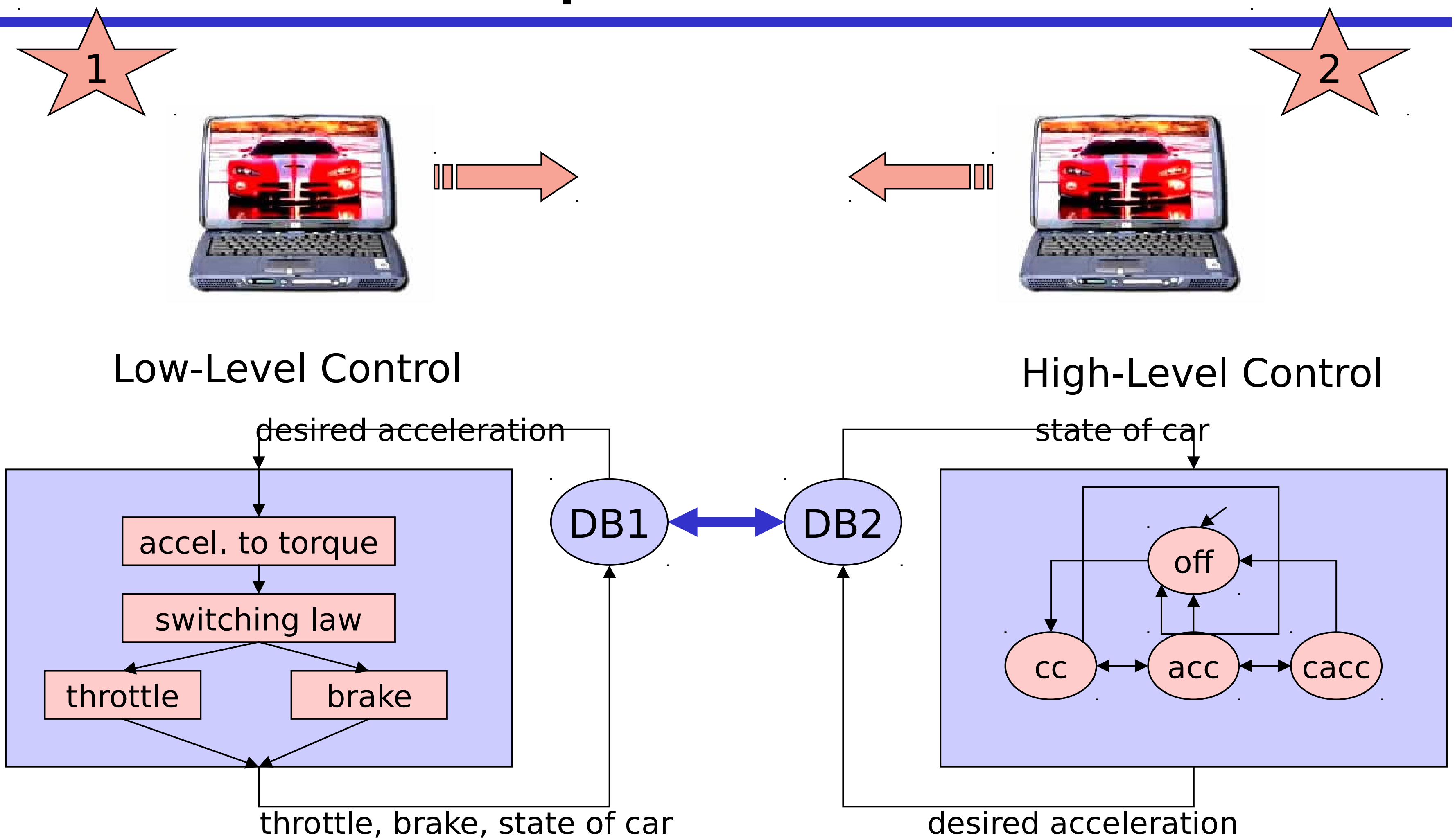
Controller Organization



Reference is http://robotics.eecs.berkeley.edu/~anouck/cdc01inv3102.p

Control Structure

Distributed P/S Database Implementation



Car make and model dependent

Car make and model independent

V2V Demos

- An suite of demos of incremental technical difficulty:
  - Low-level control done
  - CC done
  - ACC ongoing
  - CACC ongoing

- In a set of different conditions:
  - High-speed (highway conditions) ongoing
  - Stop-and-go (slow speeds) and on curved roads (controlled conditions) ongoing

Tools in the Automotive OEP

	Modeling	*Simulation*	*Analysis*	*Code Generation*	*Scheduling*
Baseline Vehicle-to-Vehicle	**Teja / C-language**	**Teja / C-language**	**-**	**Teja / C-language**	**Teja**
Baseline Powertrain	**Simulink / Stateflow**	**Simulink / Stateflow**	**-**	**Realtime Workshop / Targetlink**	**Simulink / Stateflow**
Phase I Tools	**GME (VanderbiltUniv.)**	**CHARON (U Penn)**	**CHARON (U Penn)**	**ECSL (Vanderbilt Univ.)**	**AIRES (U Mich)**
	Ptolemy	**Ptolemy**	**Checkmate (CMU)**	**Kestrel**	**Timewiz (CMU)**

HSIF will aid in tying together modeling, simulation and analysis

V2V Baseline Tool Chain

Modeling

Full car model
Controllers
Sensor Fusion

Hybrid systems
Written in the
TEJA input
language

Model Analysis

Simulation runs
conducted in
TEJA

Controller
development
and code testing

Implementation

Code generated
by TEJA
C++ chosen
(C also possible)

Sensor Fusion
(written in C)

Testing on HW

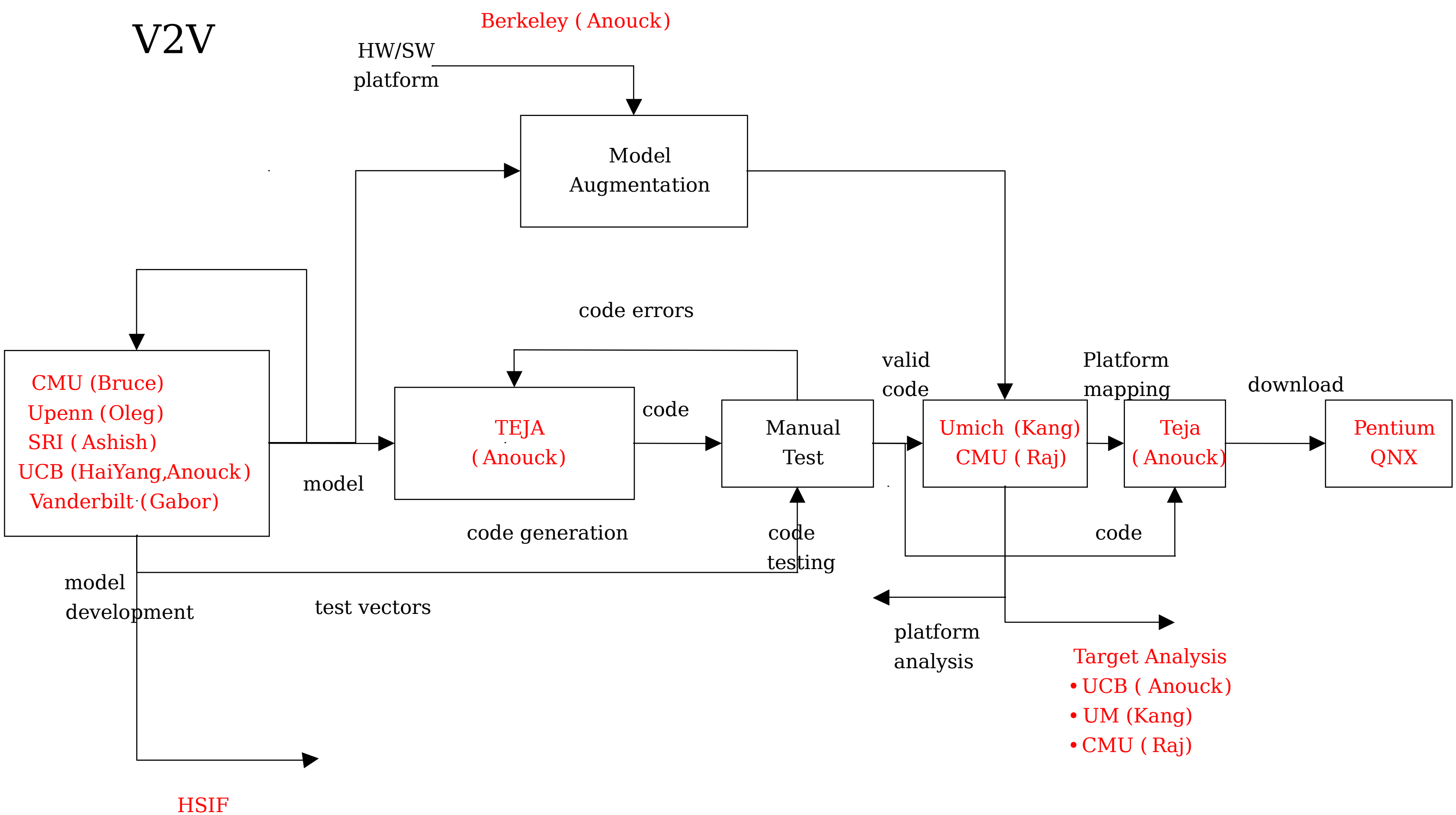
Platform

QNX RTOS
P/S database

Model
Augmentation
Schedulability
Analysis

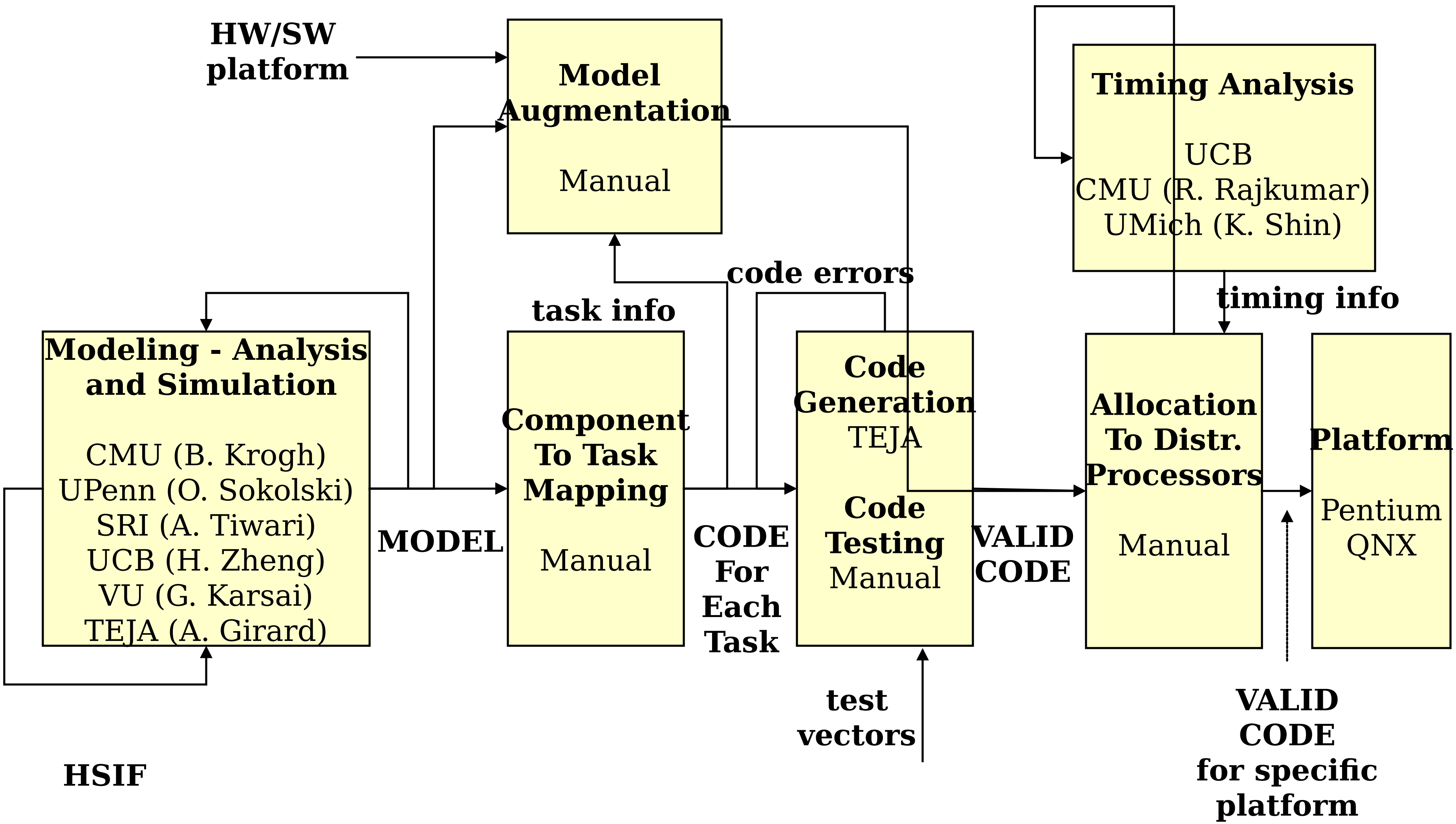
Profiling (TEJA)

V2V Process


V2V
Berkeley (Anouck)
HW/SW
platform
Model
Augmentation
code errors
CMU (Bruce)
Upenn (Oleg)
SRI (Ashish)
UCB (HaiYang,Anouck)
Vanderbilt (Gabor)
model
TEJA
(Anouck)
code
Manual
Test
valid
code
Umich (Kang)
CMU (Raj)
Platform
mapping
Teja
(Anouck)
download
Pentium
QNX
code generation
code
testing
code
model
development
test vectors
platform
analysis
Target Analysis
• UCB (Anouck)
• UM (Kang)
• CMU (Raj)
HSIF

V2V Process

UCB OEP Point of Contact: Anouck Girard (anouck@eecs.berkeley.edu)



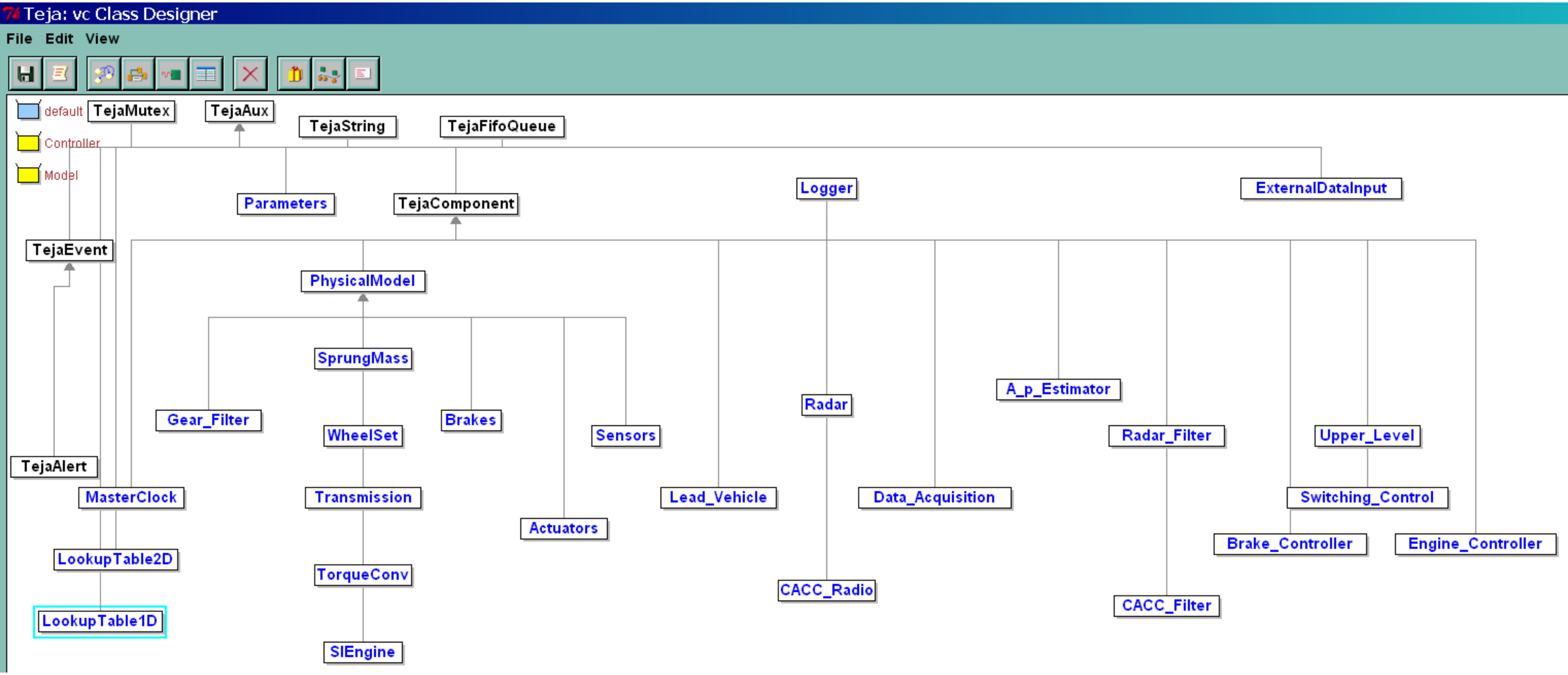
Phase I Interactions

- Worked tightly with CMU (R. Rajkumar's group) on timing issues and schedulability analysis for the vehicles.
  - UCB collected detailed measurements on our task sets on the QNX platform.
  - Timing analysis was done with CMU's assistance.
  - One task (out of about 30) was found to be unschedulable.
  - A straightforward fix is possible.
  - When all these tools integrate in a single environment, finding and fixing problems will be efficient and cost-effective!

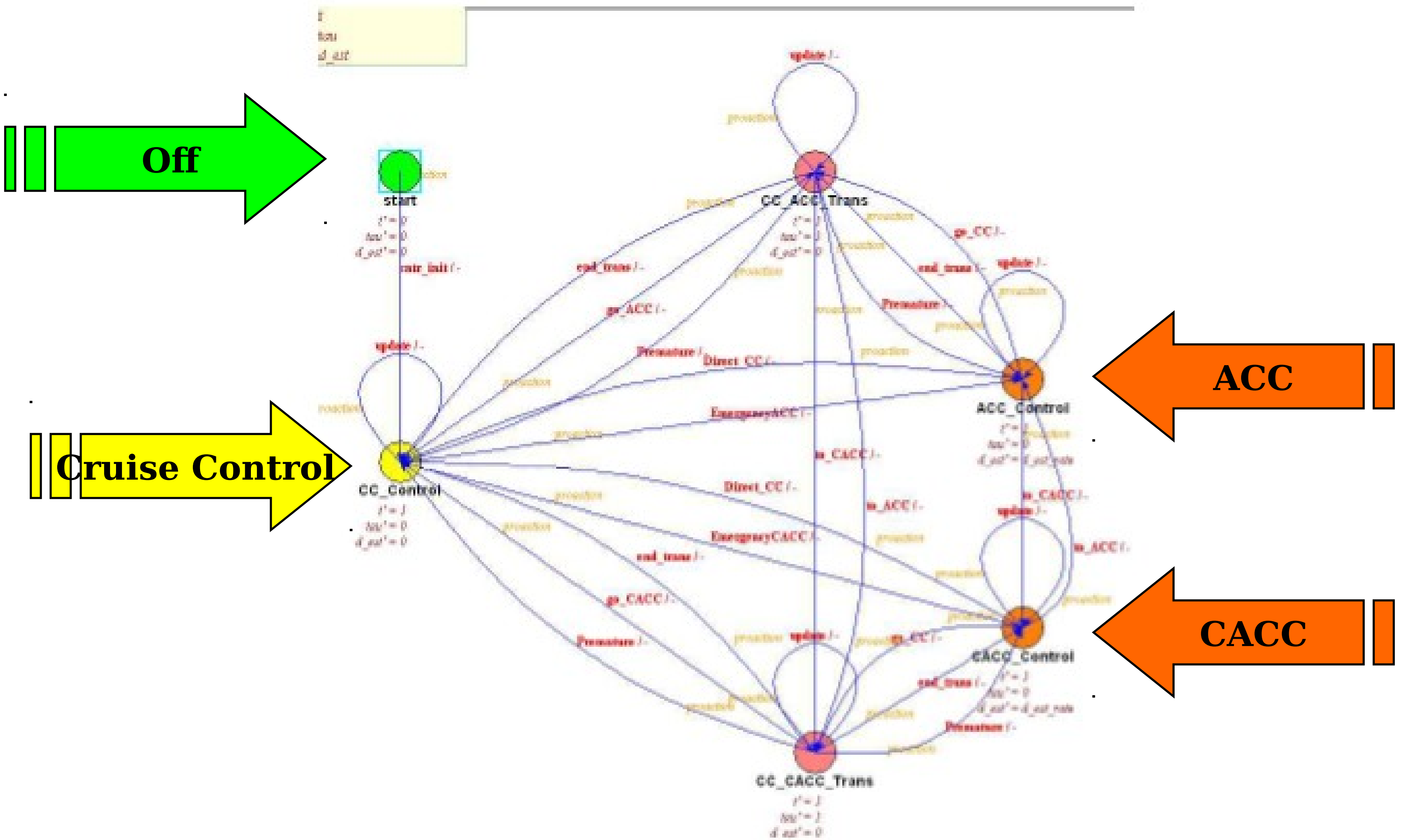
- HSIF, which is being developed as an interface to the analysis tools, is progressing quickly. Version 1.0 of the semantics is on the web (VU). A subgroup is working on defining the syntax. UCB is developing a V2V OEP related example to use as common ground between all participants.

- Are developing simpler V2V models for analysis.

TEJA V2V Components



TEJA Mode Switching



Experimental Data

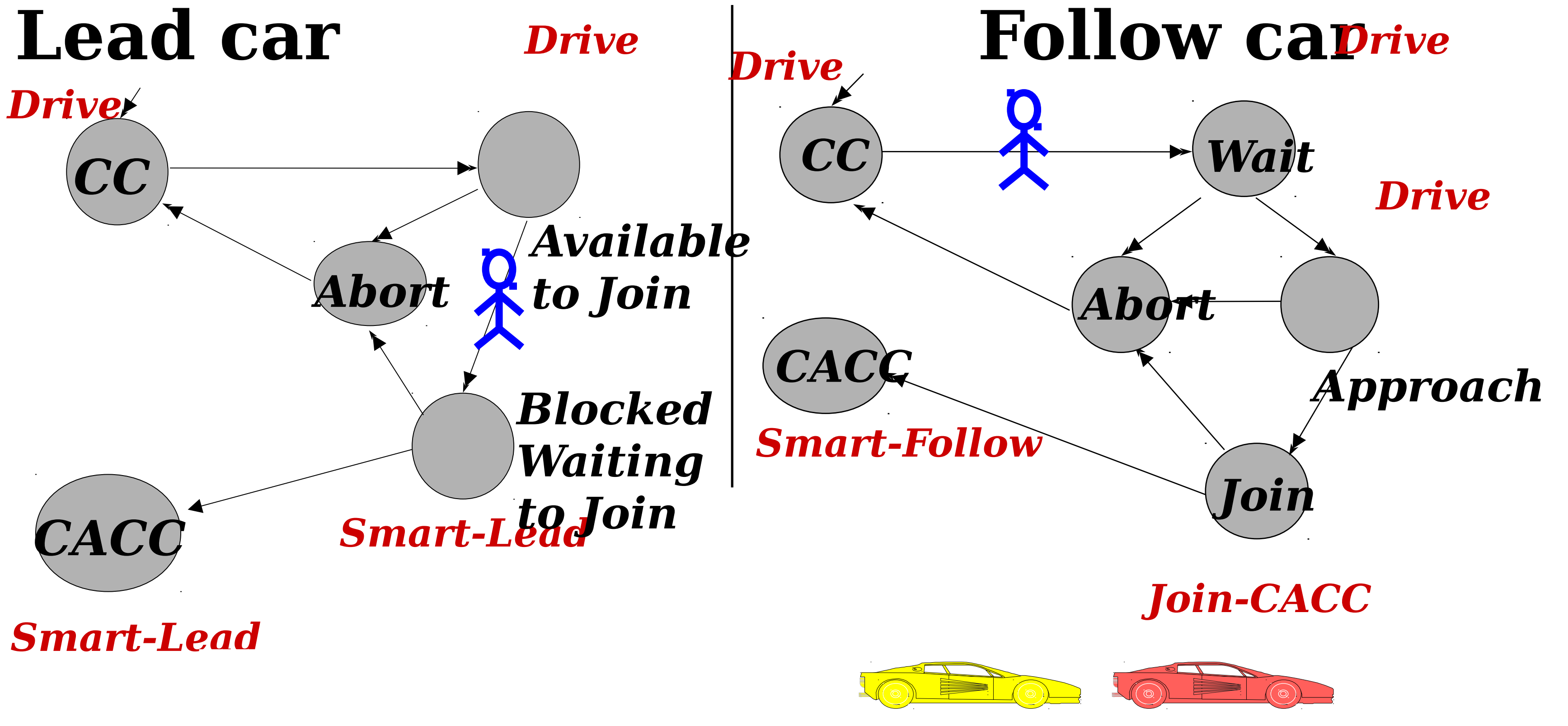
- Communication system performance
- Clock drift
- Radar and communication fusion
- CACC results at RFS
- Stop-and-go ACC video

Challenge Problems That Could Be Addressed *(and Berkeley Contacts)*

- **Modeling:**
  - Wireless communication models *(P. Varaiya)*
- **Model Analysis:**
  - Verification *(T. Simsek)*
  - Synthesis of switching laws *(T. Simsek)*
  - Performance *(K. Hedrick)*
- **Implementation**
  - Test vector generation *(T. Simsek)*
  - Schedulability analysis *(T. Simsek)*
  - Code generation *(A. Girard, M. Drew)*
  - Code debugging and testing *(A. Girard, M. Drew)*
  - Allocation to distributed platforms *(A. Girard)*
- **Integration** *(A. Girard, M. Wilcutts)*
  - Model translation (to/from TEJA)
  - Integration of different models of computation (enhance P/S inter-process comm. capabilities)
  - Tool integration (powertrain in Matlab/OSEK + vehicle to vehicle in TEJA/QNX)

Model Analysis

Verification
Example: Join cruise control maneuver



Verify that there is no collision, that is that the distance between car 1 and car 2 is greater than zero at all times.
Berkeley baseline is reachability analysis using λ-Shift.

Expanded Challenge Pb: Verification

- Verify a “mixed model”, that is expressed as a hybrid system but uses a look-up table and some experimental data as part of the model.

- In the V2V setting this experimental data may be an engine map.

Implementation
Schedulability Analysis

- **Objective: verify that implementation meets a set of timing constraints.**
- **Different techniques are applicable:**
  - **Classical schedulability analysis.**
  - **Model checking.**
  - **…**

Berkeley baseline: two solutions:

- **(Non-automated) Schedulability analysis (extended Rate Monotonic Analysis)**

  http://vehicle.me.berkeley.edu/mobies/vehicle/papers/pub-sub.pdf

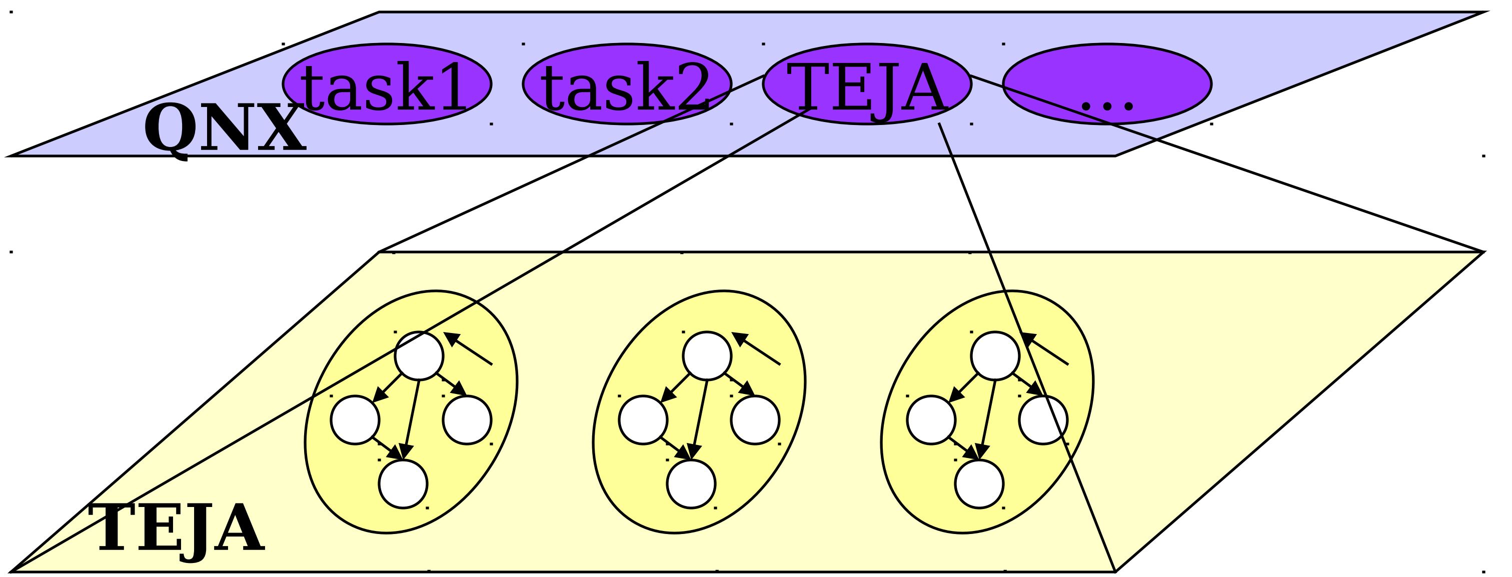
- **Model checking using a combination of CNET 's Esterel compiler Saxo-RT and the timed-automata model-checker Kronos:**

  http://vehicle.me.berkeley.edu/mobies/vehicle/papers/taxys-cdc.pdf

Expanded Challenge Pb: Schedulability Analysis

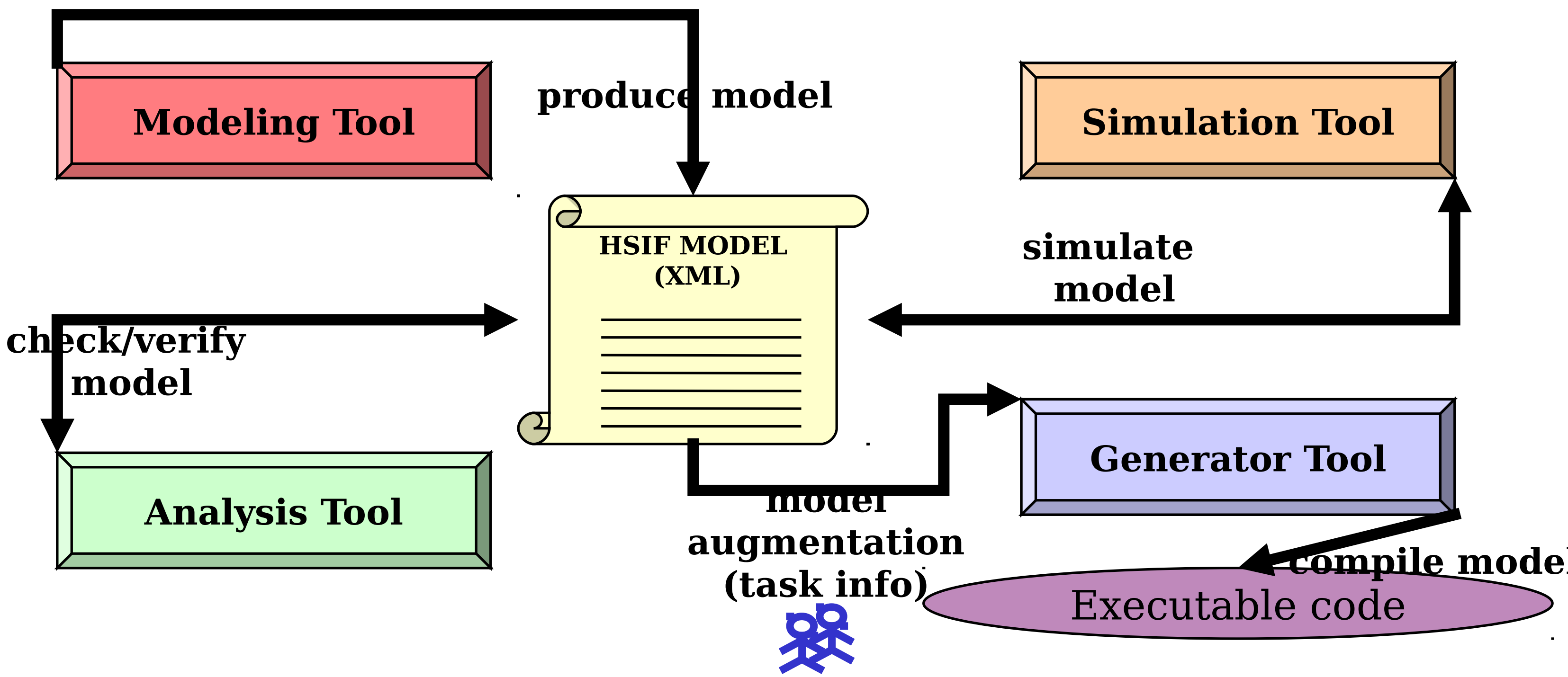
- Check schedulability properties for a "hybrid" scheduling problem, that is a two-level problem for example.

- In the V2V setting, this is equivalent to checking that not only are all the QNX tasks schedulable, but also that all the components within TEJA are schedulable.



Expanded Challenge Pb: Integration and HSIF Development

- Develop a TEJA to HSIF translator.
- Test it on a simple TEJA model.

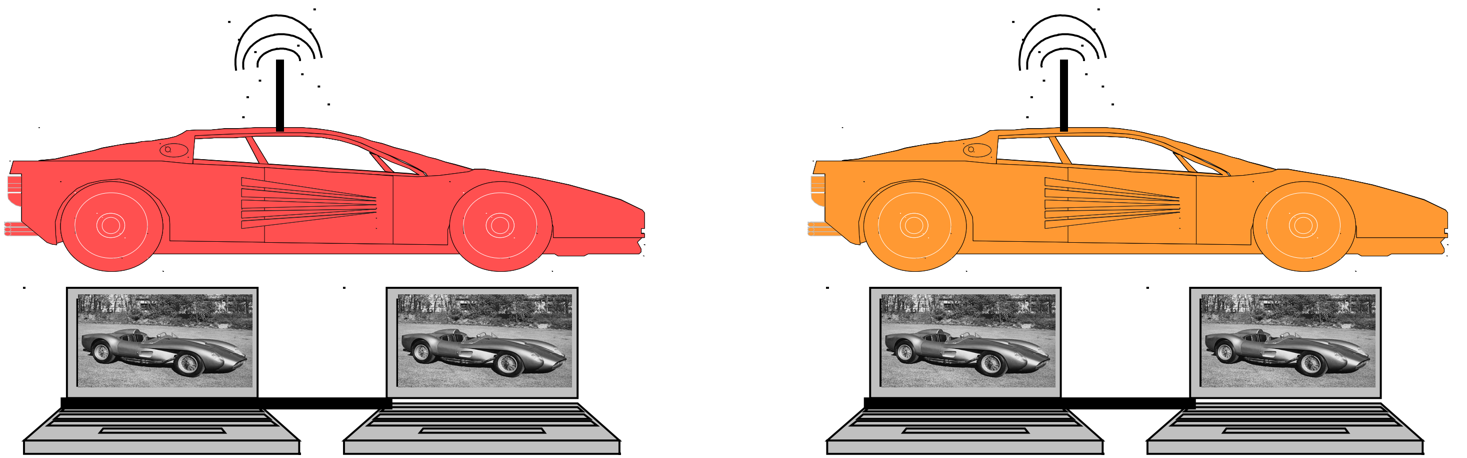


Expanded Challenge Pb:

Clock Synchronization

Clock synchronization algorithms: provide algorithm for synchronization of both computers on one car, then for synchronization of all four computers (on two cars).

Berkeley baseline will consist of two PC computers by car, communicating through a QNX P/S architecture.



Expanded Challenge Pb:

Code Generation

"Automatic code generation using commercially available tools has been a reality for over a decade. **The challenge remains to generate efficient, embedded code that is configurable and linkable to legacy code in a production environment." (Ford baseline report)**

Berkeley baseline will consist of TEJA generated code, interfacing with the rest of the vehicle hardware and software tasks through a publish and subscribe database.